UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208

25299 7590 10/25/2007
IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
10/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/771,472	**Applicant(s)** CALVIGNAC ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

ELLEN TRAN
PATENT EXAMINER
ART 2134

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 13 August 2007, with acknowledgement of an original application filed 26 January 2001.

2. Claims 1-20 are currently pending in this application. Claims 1, 16, and 19 are independent claims.

Response to Arguments

3. Applicant's arguments with respect to 1-20 have been considered but they are moot due to new grounds of rejection below or not persuasive where noted below.

I) In response to Applicant's argument beginning on page 7, *"However, the Examiner is not correct that KAPLAN teaches a combination logic comprising logic functions whose output depend solely on their inputs and utilizing logic circuits without memory ... While such language discusses parallel execution and sequential processing of Encrypt-then-Hash and Decrypt-then-Hash operations, such language is silent with regard to a combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory. (claims 1, 16, and 19)".*

The Examiner disagrees with argument for multiple reasons. The Applicant is reminded the reference should be reviewed for all it contains. In addition the portion in Kaplan indicates "hardware accelerated", the Examiner interprets this to have the same meaning as 'logic circuits without memory'.

The Examiner agrees with applicant concerning claims 5-8 and the rejection below has been amended.

The Examiner recommends the following amendment to independent claim 1, it is also recommended that the other independent claims be amended similar to the shown amendment. The added features are from Applicant's specification and drawings.

Claim 1 - A hardware implementation of a crypto-function comprising:

a first register storing data to be encrypted or decrypted;

wherein the inputs to the first register are bits from an initial value accumulator, a data register, and a key register;

~~a second register for receiving data which has been encrypted or decrypted; and~~

combination logic performing computational iterations of the crypto-function on data stored in the first register wherein the outputs that are inputs to subsequent iterations are processed without being stored in intermediate registers; ~~and outputting data to said second register in a single hardware cycle,~~

the bits from the initial value accumulator and the data register are exclusive ORed and then subjected to an initial permutation, IP in permutation logic;

the IP logic consists of two outputs that are wire only, the results are not stored in intermediate result registers;

wherein one of the IP logic output is input to a cipher function that performs a key-dependent computation which involves the key schedule which is a computed from the input key register;

wherein the second IP logic output is exclusive ORed with the result of the key-dependent cipher function;

wherein the combination logic with the IP logic and the key-dependent cipher are repeated a pre-determined number of iterations;

wherein the combination logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory.

Specification

4. The disclosure is objected to because of the following informalities: in Applicant's specification paragraph 0008, from the publication 2002/0101985 the following is indicated:

> "In one implementation of the invention, the Data Encryption Standard (DES) algorithm is implemented in combinational logic which performs the encryption or decryption in one hardware cycle. The DES algorithm, as set forth in Federal Information Processing Standards Publication FIPS PUB 463, as reaffirmed Oct. 25, 1999, from the National Institute of Standards and Technology of the U.S. Department of Commerce, is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key. A block to be enciphered is subjected to an initial permutation and then to a complex key-dependent computation and finally a permutation which is the inverse of the initial permutation. Deciphering is accomplished by using the same key as for enciphering, but with a schedule of addressing the key bits altered so that the deciphering process is the inverse of the enciphering process. The computation which uses the permuted input block as its input to produce the pre-output block consists, but for a final interchange of blocks, of sixteen iterations of a calculation which operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits. In prior hardware implementations, registers are required to store the intermediate results of these sixteen iterations requiring sixteen clock cycles to accomplish the computations, but the combinatorial logic used to implement the algorithm according to the teachings of the present invention perform the computations in one hardware cycle that is approximately ten clock cycles" .

The Examiner objects because the correct FIPS PUB is 46-3 not "463" as indicated. In addition although the FIPS PUB 46-3 was reaffirmed in Oct. 25, 1999 it was then withdrawn in May 2005. Therefore, it is recommended that "as reaffirmed Oct. 25, 1999" be deleted from the specification. Furthermore it is well known in the art that the DES key consists of 56 bits. Appropriate correction is required.

Drawings

5. The drawings are objected to because:

A) The specification was not updated to indicate the drawings submitted 6 February 2002, which have FIG. 1A, FIG. 1B, FIG. 2A, and FIG. 2B.

B) The drawings appear to be informal, the number are missing as indicated in the specification 101 from FIG. 1 as well as 201, 202, 203, from FIG. 2.

Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for

> patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

7. **Claims 1-4 and 9-20** are rejected under 35 U.S.C. 102(e) as being anticipated by Kaplan et al. U.S. Patent No. 6,704,871 (hereinafter '871).

As to independent claim 1, "A hardware implementation of a crypto-function comprising:" is taught in '871 col. 2, lines 16-18, note the security functions described are 'crypto-function' and the circuit is the 'hardware implementation';

"a first register storing data to be encrypted or decrypted; a second register for receiving data which has been encrypted or decrypted" is shown in '871 col. 11, lines 16-25, note the registers that facilitate bidirectional communication are interpreted to be the first register, i.e. input and second register, output;

"and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle" is disclosed in '871 col. 10, lines 14-25;

"wherein the combinational logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory" is taught in '871 col. 10, lines 26-44, note the combined operations that operate in parallel off of the same source is interpreted to be combinational logic without memory.

As to dependent claim 2, "wherein the crypto-function is a block cipher algorithm" is taught in '871 col. 10, lines 15-17.

As to dependent claim 3, "wherein the crypto-function is the Data Encryption Standard (DES) algorithm" is shown in '871 col. 10, lines 15-17.

As to dependent claim 4, "wherein the crypto-function is the CHAIN algorithm" is disclosed in '871 col. 10, lines 15-17.

As to dependent claim 10, "wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers" is disclosed in '871 col. 10, lines 15-17.

As to dependent claim 11, wherein the hardware implementation the crypt-function computes an iterated round function in one clock cycle" is taught in '871 col. 10, lines 15-17.

As to dependent claim 12, "wherein the combination logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combination logic" is shown in '871 col. 10, lines 15-17.

As to dependent claim 13, "wherein the combination logic utilizes logic functions whose outputs depend solely on their inputs" is disclosed in '871 col. 10, lines 15-44.

As to dependent claim 14, "wherein the combination logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of encipher or deciphering computations" is taught in '871 col. 10, lines 15-44.

As to dependent claim 15, "wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read" is shown in '871 col. 10, lines 15-44.

As to independent claim 16, "A hardware implementation of a crypto-function comprising:" is taught in '871 col. 2, lines 16-18

"a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted" is shown in '871 col. 11, lines 16-25;

"and combinational logic that performs computation iteration of the crypto-function on data store in the first register and outputting data to said second register in a single hardware cycle, the combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory, wherein the crypt-function without intermediate registers that require loading and settling time before contents of the intermediate registers can be read" is disclosed in '871 col. 10, lines 14-44.

As to dependent claim 17, "wherein the single hardware cycle is approximately ten clock cycles" is disclosed in '871 col. 10, lines 13-25,

As to dependent claim 18, wherein the hardware implementation of the crypto-function computes and iterated round in just one clock cycle" is disclosed in '871 col. 22, lines 48-55.

As to independent claim 19, "A hardware implementation of a crypto-function comprising:" is taught in '871 col. 2, lines 16-18;

"a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted" is shown in '871 col. 11, lines 16-25;

"and combination logic that performs computation iteration of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle, the combination logic comprising logic functions whose outputs depend

soley on their inputs and utilizing logic circuits without memory, wherein the single hardware cycle comprises several clock cycles" is disclosed in '871 col. 10, lines 14-44.

As to dependent claim 20, "wherein the cypto-function is implemented in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read" is shown in '871 col. 10, lines 14-44.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 5-8,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan et al. U.S. Patent No. 6,704,871 (hereinafter '871) in view of Greene U.S. Patent No. 6,870,929 (hereinafter '929).

As to dependent claim 5, the following is not explicitly taught in '871: **"wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times"** however '929 teaches "A scheduler 106 can be programmed to provide appropriate priority to ensure feedback-type encryption operations. In particular, the active contexts can be stored, and on consecutive cycles, priority can be shifted to give the desired context priority. As shown in FIG. 4A, at time t14, priority can be shifted to give data block E1 priority. Further, one skilled in the art would recognize that the feedback loop in an encryption circuit would be disabled on this cycle to prevent the E.sub.KB [B3] value from being combined with the E1 value" in col. 7, lines 7-21 and col. 7, line 62 through col. 8, line 4.

It would have been obvious to one of ordinary skill in the art at the time of the invention cryptographic co-processor taught in '871 to include a means to utilize a different cipher function such as invertible key dependent rounds. One of ordinary skill in the art would have been motivated to perform such a modification because stronger flexible algorithms are needed for security see '1929(col. 3, lines 29-45) "In light of the various applications for encryption circuits, only a few of which are mentioned above, there is a need for encryption systems that can process data blocks with higher throughput. Other types of data operations can present problems which are similar in nature to encryption functions. For example, many operations can have "feedback" type steps, where a computed value is fed back into a computation stage as an operand. One particularly useful type of operation is modular exponentiation. In modular exponentiation, the computation can be reduced into a number of smaller multiplication and modular reduction steps, allowing for faster implementation on a computer or other hardware".

As to dependent claim 6, "wherein the combination logic performs mixing, permutation and key-dependent substitution in each round" is shown in '929 col. 7, lines 7-21 and col. 8, lines 6-32.

As to dependent claim 7, "wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-

dependent computation followed by a permutation which is an inverse of the initial permutation" is disclosed in '929 col. 7, lines 51-67.

As to dependent claim 8, "wherein the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process" " is taught in '929 col. 10, lines 8-17.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran

Ellen Tran
Patent Examiner
Technology Center 2134
18 October 2007